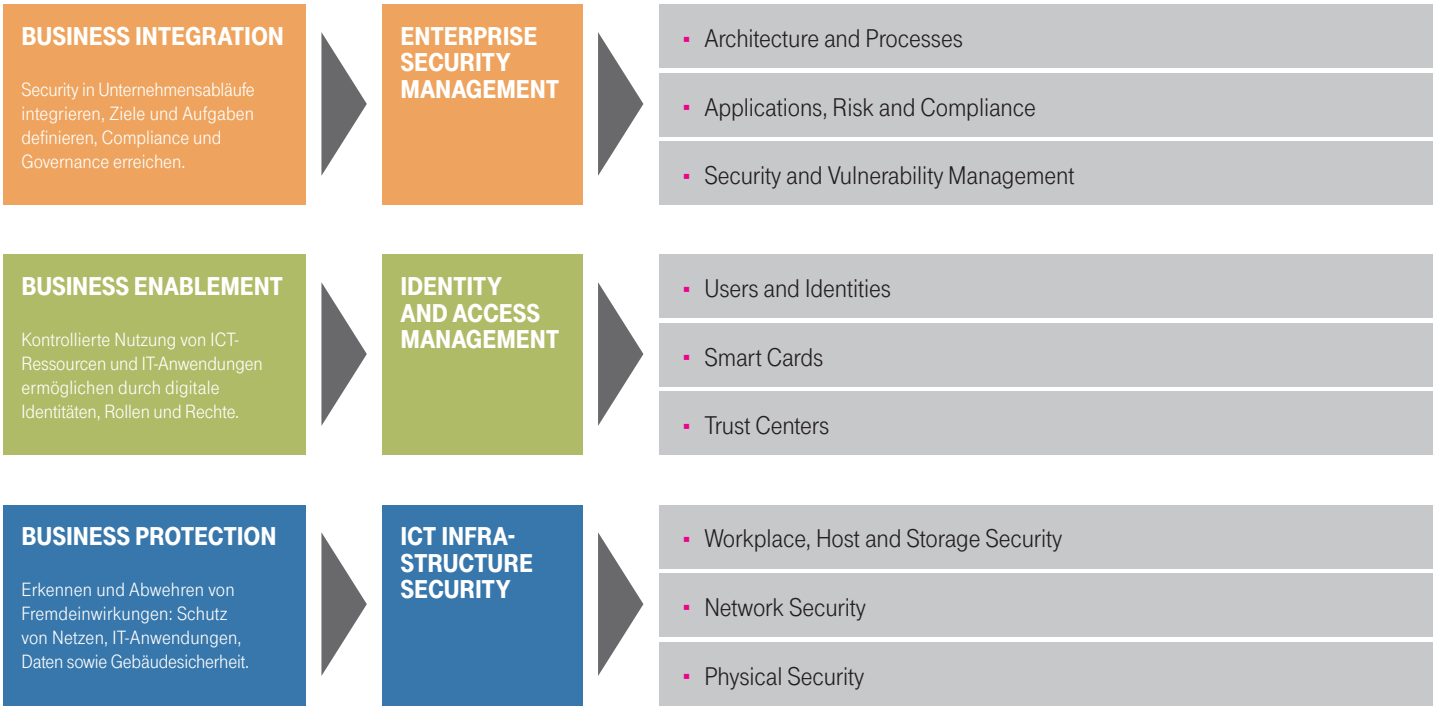
ICT SECURITY SERVICES

Die Support & Enabling Services ergänzen und komplettieren das Portfolio von T-Systems. Onsite Services unterstützen Kunden in der Fläche und vor Ort mit standardisierten ICT-Lösungsbausteinen (Service Cluster). Mit den Service Desk Services erhält der Kunde eine konsistente Betreuung mit ein und demselben Ansprechpartner während der gesamten Anfrageabwicklung. Transparenz und Optimierung der ICT-Infrastruktur und -prozesse sind eine ständige Aufgabe. Mit Application Performance Management wird ein durchgängiges Analyse- und Monitoring-Werkzeug bereitgestellt, das die kritischen Geschäftsprozesse des Kunden aus Benutzersicht darstellt. ICT Security Services von T-Systems helfen Unternehmen, der immer wachsenden Gefährdung durch Cyber-Angriffe zu begegnen.

Die Anforderungen von Unternehmen an Sicherheit verändern sich rasant. Einerseits müssen sie unberechtigte Einwirkungen auf Systeme und Daten ausschließen, andererseits soll der Datenzugriff von innen sowie außen definiert und kontrolliert möglich sein. Ließen sich Netzwerke, Systeme und Anwendungen bisher noch mit singulären Security-Angeboten schützen, so ist heute eine ganzheitliche Betrachtung des Unternehmens und seiner Prozesse notwendig. Dabei müssen IT und TK integriert gesehen werden. Auf Organisationsebene kommen weitere Aspekte hinzu: Steuerungsfähigkeit (Governance), Risikomanagement, Unternehmenskultur und Organisationsmodelle (Risk) wie auch die Einhaltung rechtlicher und regulatorischer Anforderungen, Verträge und eigener Richtlinien (Compliance). Ein übergreifendes Sicherheitsmanagement bündelt diese Anforderungen unter einem Dach. ICT Security Services bieten ganzheitliche, dennoch modulare Sicherheitslösungen, die Ihr Geschäft nach Ihren individuellen Anforderungen optimal unterstützen.

T · · Systems ·

SICHERHEIT VON DER PLANUNG ÜBER DIE REALISIERUNG BIS ZUM BETRIEB



ICT SECURITY SERVICES – OFFERING-ELEMENTE

Sie erhalten umfassende Beratungsleistungen zu allen Themen – von der Ebene der Geschäftsprozesse über Security Policys und Sicherheitskonzepte bis hin zur Umsetzung. T-Systems testet die erreichte Sicherheit, führt Bedrohungs- und Risikoanalysen durch, entwirft Architekturen sowie Lösungen und erstellt detaillierte Maßnahmenkataloge. Dazu kommt die Implementierung eines Information Security Managements, z. B. nach ISO 27001.

1. ENTERPRISE SECURITY MANAGEMENT

Security muss heute als Teil des operativen Risikomanagements verstanden werden. Die Durchsetzung definierter Grundsätze und Standards zum Schutz von Geschäftsprozessen, Organisation und ICT-Systemen verlangt eine Verankerung in den Unternehmensprozessen der Organisation. Technische Maßnahmen werden in einem mehrstufigen Verfeinerungsprozess konzipiert und implementiert. Mit ihrer Umsetzung stellen Sie die Einhaltung aller selbst definierten Richtlinien und öffentlichen Regularien sicher.

Architecture and Processes: Definiert Grundsätze, Standards sowie Prozesse und bildet den Rahmen für die entsprechenden Systeme. Ein Projekt- und Programm-Management bietet den notwendigen strukturellen Rahmen. Design und Entwicklung von Architekturen, Security-Konzepten, Systemen und Software für diverse Anwendungsszenarien, z. B. spezifische Key-Management-Lösungen.

Applications, Risk and Compliance: Dient der Identifikation und Bewertung von Risiken und der Konzeption von Maßnahmen. Die Organisation wird auditiert und alle Anwendungen werden abgesichert. Eine Prüfung der Systeme und Produkte hilft, Sicherheitslücken von vornherein zu vermeiden und gesetzliche Vorgaben z. B. an Datensicherheit und Governance zu erfüllen.

Security and Vulnerability Management: Um Gefährdungen auszuschließen, müssen diese zunächst erkannt und bewertet werden. Im nächsten Schritt werden Maßnahmen erarbeitet, wie auf Sicherheitsvorfälle zu reagieren ist. ICT-gestütztes Compliance Reporting, Lagebilder und die Forensik helfen dabei, Bedrohungen zu verhindern.

2. IDENTITY AND ACCESS MANAGEMENT

Interne und externe Kooperationen werden in einer vernetzten Welt immer intensiver und komplexer – Grenzen verschwinden. Mit Identity and Access Management (IAM) schaffen Sie die Voraussetzung, um ICT-Ressourcen und IT-Anwendungen kontrolliert zu nutzen. Kern dieser Lösung sind digitale Identitäten, Rollen und Rechte für den sicheren Zugriff auf Geschäftsprozesse im Unternehmen und darüber hinaus. Outsourcing und Cloud Computing (Dynamic Services) sind ohne geregelte Zugänge nicht realisierbar. Mit IAM erreichen Sie auch die notwendige Flexibilität und Produktivität bei Veränderungsprozessen im Unternehmen.

Users and Identities: Indem Sie digitale Identitäten einrichten, Rechte definieren und automatisiert prüfen, können Sie ICT-Ressourcen kontrolliert nutzen.

Smart Cards: Chipkarten sind Sicherheitsmodule und Organisationsmittel in einem. Diese Alleskönner im Miniformat werden für Basis- wie auch Individualfunktionen verwendet, z. B. für Identifikationssysteme.

Trust Centers: Die sichere Erzeugung und Prüfung von digitalen Identitäten ist die Basis für Verlässlichkeit und Vertrauen. Nutzen Sie die PKI-Technologie (Public Key Infrastructure), um Nachrichten digital zu signieren und zu verschlüsseln – entweder als Service oder als eigenes System. SSL-Zertifikate sichern die Datenübertragungen ab.

3. ICT INFRASTRUCTURE SECURITY

Unternehmen müssen ihre ICT-Infrastrukturen abschirmen, Angriffe auf Systeme, Anwendungen und Netze erkennen sowie Daten und Datenströme schützen. Die zunehmende Mobilität verlangt flexible Lösungen für die sichere Verbindung zu Unternehmensnetzen und -anwendungen und die sichere Übertragung von Daten. Sie erhalten Lösungen, die Ihre ICT-Systeme schützen, Datenströme filtern und selbst Informationsflüsse kontrollieren und steuern. Zum Einsatz kommen VPN- und Firewall-Lösungen, Antivirus-, Anti-Spam- und andere Filterlösungen, Intrusion Detection and Prevention ebenso wie Lösungskomponenten für Mobilität und sichere Kommunikation.

Workplace, Host and Storage Security: Anwender verarbeiten ihre Daten lokal und greifen von ihrem Arbeitsplatz aus übers Netz auf Server zu. Kontrolle und Schutz sind an mehreren Stellen wichtig: Content Security, Encryption (Verschlüsselung von Daten und Hardware), Secure Virtual Workplace und Device Security. Die Daten werden auf Servern verarbeitet und gespeichert. Die Integrität der Systeme und der Schutz der Services sind essenziell. Wesentliche Schutzmechanismen bilden Content Security (Host), Managed Anti-Spam Services (Cloud Service) und Security Application Services.

Network Security: Netzwerke verbinden Applikationen und Nutzer und transportieren alle Daten. Sie sind das Einfallstor für Angriffe und die zentrale Stelle für Sicherheit. Das Angebot gliedert sich nach technischen und funktionalen Management-, Provisioning-, Maintenance- und Professional-Modulen. Dahinter verbergen sich Lösungen und Services, die unberechtigte und arglistige Zugriffe und Interaktionen mit den IT-Komponenten in Ihrem Netz verhindern. NSS bieten eine sichere Verbindung Ihres Intranets zum Internetverkehr, aber auch zwischen verbundenen Unternehmen, Niederlassungen oder Abteilungen.

Physical Security: Umfasst Lösungen für die Gebäudesicherheit, von Videoüberwachung über Zutrittskontrolle, Einbruch- und Brandmeldetechnik bis hin zu Leitstellenservice.
Es werden technisch-funktionale Leistungsmerkmale mit Ihren individuellen Managementmodulen gebündelt. Dabei gibt es folgende Funktionsblöcke: Network-Transport-Schutzmechanismen, Content-Security-Schutzmechanismen, Betriebsleistungen, Bereitstellungsleistungen, zugehörige Maintenance Services und Projektierungsleistungen.

ALLE VORTEILE IN DER ÜBERSICHT

NUTZEN
Sie erhalten Unterstützung in allen Phasen einer komplexen Systemrealisierung nach dem Prinzip „Plan – Build – Run“.
Ihr Vorteil ist die durchgängige Sicherheit Ihres Systems entsprechend des vereinbarten Servicelevels.
Sie erhalten Mehrwert „end-to-end“ entlang Ihrer gesamten Wertschöpfungskette. Ihr Nutzen liegt in der Prozessoptimierung, Kostensenkung und Verbesserung der Ergebnissituation.

WACHSTUMSEFFEKTE
- Sie erhalten flexible Geschäftsabläufe durch mobile und übergreifende Verfügbarkeit von Daten und Anwendungen
- Sie können neue Online-Geschäftsmodelle etablieren durch sichere Identifizierung und Zusammenarbeit
- Sie können Ihre Unternehmensstrukturen schnell und sicher den Markterfordernissen anpassen

KOSTENEFFEKTE
- Investitionsschutz von Know-how und ICT-Infrastrukturen
- Vermeidung von Kosten durch Betriebsstörungen
- Vermeidung von Schäden durch Gesetzesverstöße und Sicherheitsvorfälle
- Kalkulierbarkeit von Unternehmensrisiken
- Qualitätssteigerung und Kostenreduktion bei der Unternehmenssicherheit durch Managed Security Services

BETRIEBSMODELLE
Als einer der großen Outsourcing-Dienstleister übernimmt T-Systems den Betrieb Ihrer Sicherheitssysteme komplett oder führt die notwendigen Arbeiten zur Administration, Aktualisierung und Pflege Ihrer Inhouse-Systeme durch (Security Management Center, Remote Management und Outtasking). Die Managed Security Services umfassen auch das Device Security Management.

INTERNATIONALE VERFÜGBARKEIT
T-System beschäftigt ca. 600 Sicherheitsspezialisten mit umfangreichen Zertifizierungen für den externen Markt und ist in 25 Ländern präsent. T-Systems betreibt international sechs Security Operation Center.

ICT SECURITY SERVICES VON T-SYSTEMS

WARUM T-SYSTEMS?

T-Systems ist in Deutschland führend im Bereich IT-/ TK-Sicherheit (englisch: ICT Security). Seit mehr als 20 Jahren unterstützen wir Behörden und Unternehmen aus allen Branchen. Sie profitieren von der in vielen Großprojekten gesammelten Erfahrung und können auf die Qualität und Objektivität der Beratung und Bewertung vertrauen. Sie erhalten umfassende Dienstleistungen auf dem Gebiet der ICT Security. Dabei betrachten wir die Organisation, Abläufe und Technik auf allen Ebenen. Sie erhalten Services entlang der gesamten Wertschöpfungskette, dazu gehören Consulting, Entwicklung / Integration, Produkte sowie der Betrieb. Sie profitieren von aufeinander abgestimmten Dienstleistungen und Lösungen, die Ihre Anforderungen in Bezug auf Sicherheit und die Einhaltung gesetzlicher Vorgaben an Governance und Compliance erfüllen.
T-Systems verfügt über Akkreditierungen des Bundesamts für Sicherheit in der Informationstechnik (BSI), von VISA International, MasterCard International, PCI und vielen anderen Organisationen weltweit.

AUSGEWÄHLTE PARTNER UND LIEFERANTEN

ZERTIFIKATE, AKKREDITIERUNGEN, QUALIFIKATIONEN

- ISO 9001
- ISO 14001
- ISO 20000
- ISO 27001
- OHSAS 18001
- PCI-DSS
- CISSP
- BSI IT-Grundschutz
- ISAE 3402
- CISM
- CISA
- CRISC
- ITIL
- T.I.S.P.

Referenzbeispiele:

EADS

- Erfüllung höchster Sicherheitsanforderungen für die Entwicklung in internationalen Hightechprojekten
- Sichere Datenkommunikation
- Variable Zugangsberechtigungen mit bedarfsgerechtem Registrierungsverfahren für Mitarbeiter
- Abgestufte Sicherheit auf Basis einer konzernweiten Public-Key-Infrastruktur

SIMKO FÜR DEN BUND

- „Sichere Mobile Kommunikation“ (SiMKo) für die Regierung und Behörden durch Ende-zu-Ende-Sicherheit vom Backend-System bis zum mobilen Smartphone
- Sämtliche Daten, Software und Betriebssystem sind verschlüsselt
- Einsatzempfehlung für den Geheimhaltungsgrad VS-NfD durch das Bundesamt für Sicherheit in der Informationstechnik (BSI)

ANVIS GROUP

- Innovatives Identity Management beschleunigt Administrationsprozesse und spart Kosten
- Erprobtes Cloud-Konzept ermöglicht unkomplizierte Benutzerverwaltung
- Lösung ist sofort einsatzbereit und für Unternehmen jeder Größe geeignet
- Einführung zum Festpreis macht sich schnell bezahlt
- Revisionssichere Protokollierung, umfassendes Reporting
- Compliance-konform, hohe Betriebssicherheit

WEITERE INFORMATIONEN
Internet: www.t-systems.de

EXPERTENKONTAKT
Bernd König
Am Propsthof 51
53121 Bonn
E-Mail: bernd.koenig@t-systems.com

HERAUSGEBER
T-Systems International GmbH
Hahnstr. 43d
60528 Frankfurt am Main
Deutschland

T · · Systems ·

Stand 11 / 2013 | Änderungen und Irrtümer vorbehalten | Papier chlorfrei gebleicht | typix